REMARKS

I. Introduction

In response to the Office Action dated February 9, 2007, claims 19-27 have been canceled, claims 1, 10 and 16 have been amended, and new claims 28-31 have been added. Claims 1-18 and 28-31 are in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. Drawing Objections

In paragraph (1), the Office Action stated that Figures 1 and 2 should be designated and labeled as prior art.

Applicants' attorney respectfully traverse these objections and requirements. Figures 1 and 2 are not prior art as they comprise a new system claimed by Applicants.

III. Specification Objections

In paragraphs (2)-(3) of the Office Action, the specification was objected to because of certain informalities.

Applicants' attorney has amended the specification to overcome these objections.

IV. Claim Objections

In paragraph (4) of the Office Action, claims 16 and 17 were objected to because of certain informalities, and claims 19-27 were objected to as being substantial duplicates of claims 10-18.

Applicants' attorney has amended claim 16 and canceled claims 19-27 to overcome these objections.

V. Prior Art Rejections

In paragraphs (6)-(7) of the Office Action, claims 1-27 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Publication No. 2001/0017920 (Son). In paragraphs (8)-(10) of the Office Action, claims 1-27 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 4,633,309 (Li) in view of "PKCS #1 v2.1: RSA Cryptography Standard" (RSA).

Applicants' attorney respectfully traverses these rejections.

The Applicants' invention, as recited in amended independent claims 1 and 10, is patentable over the references, because it contains limitations not taught by the references. None of the

references, taken individually or in combination, teach the same combination of elements as Applicants' claims.

The Office Action, on the other hand, asserts that all the elements of the independent claims are shown in Son and the combination of Li and RSA.

However, when placed in context, these portions of the Son, Li and RSA references omit novel elements of Applicants' invention. Consider that Applicants' independent claims recite that the host-client pairing key, which is used to encrypt a copy protection key used to encrypt and decrypt the program materials when shared between the host and client receivers, is generated by the service provider and shared between the host receiver and client receiver in order to share the program materials between the host receiver and client receiver, wherein the service provider establishes the host-client pairing key for a particular combination of the host and client receivers. None of the references teach or suggest this aspect of Applicants' claims.

First, it is noted that Son does not teach or suggest host and client receivers. Instead, Son describes a video on-demand source and remote server, which are part of the distribution system, transmitting a video program to a subscriber station. Moreover, Son merely describes how the remote server, which obtains the video program from the video on-demand source, provides the video program to a subscriber station.

For example, FIG. 5B of Son depicts a secure process for distributing video on-demand content, which is termed a decrypt, re-encrypt, and store process. The video program is encrypted by the video on-demand source, and then transported to the remote server within the distribution center. The remote server decrypts the video program from its first encrypted form using a key received from the video on-demand source. The remote server then re-encrypts the video program into a second encrypted form using a second key, wherein the re-encrypted program in the second encrypted form (and the second key if necessary) is distributed to the requesting subscriber stations. At the subscriber stations, the re-encrypted program in the second encrypted form is decrypted using the second key, and displayed on a television monitor connected to set-top box.

However, nowhere does Son describe a host-client pairing key that is used to encrypt a copy protection key used to encrypt and decrypt the program materials when shared between the host and client receivers, wherein the host-client pairing key is generated by the service provider and shared between the host receiver and client receiver in order to share the program materials between the host receiver and client receiver, and the service provider establishes the host-client pairing key for a particular combination of the host and client receivers.

Second, it is noted that Li merely describes a method of controlling the operation of slave decoders in a cable television distribution system having a central control computer, in which each subscriber location having a slave decoder also has a master decoder. In Li, control messages for the slave decoders are transmitted to the master decoders, which retransmit the control messages to its associated slave decoders.

However, as admitted by the Office Action, Li does not teach or suggest the use of cryptography. Therefore, the Office Action also cites RSA as teaching various cryptographic methods. Nonetheless, nowhere does the combination of Li and RSA teach or suggest a host-client pairing key, which is used to encrypt a copy protection key used to encrypt and decrypt the program materials when shared between the host and client receivers, that is generated by the service provider and shared between the host receiver and client receiver in order to share the program materials between the host receiver and client receiver, wherein the service provider establishes the host-client pairing key for a particular combination of the host and client receivers.

Instead, Li merely describes that the central control computer can individually address and individually control each master decoder and each slave decoder. Control messages are sent from the central control computer at a frequency of 105.4 MHz. These signals are only receivable at each master decoder, as each slave decoder, although originally identical to a master decoder, is programmed, once installed, to only receive control messages at a different frequency, namely 10.7 MHz. Each master decoder retransmits any message to an associated slave decoder at the different frequency, 10.7 MHz. Thus, a control message destined for slave decoder will be transmitted on the cable system at a frequency of 105.4 MHz and, accordingly, will be received at master decoder. This same message will be immediately retransmitted from master decoder to the slave decoder. However, this message is not received by the slave decoder, because it is not transmitted at 10.7 MHz. Thus, in a legitimate master/slave decoder location, the slave decoder cannot receive control messages other than those which are retransmitted from its master decoder.

Li envisions that, in the event that an unauthorized slave decoder is connected to the cable system, and it is connected to receive a control channel message at 105.4 MHz, the system is arranged so that such an unauthorized slave decoder will be decommissioned or deauthorized. Periodically, the central control computer sends deauthorization messages addressed to all slave decoders as a group. These signals are sent at the control message frequency of 105.4 MHz.

However, preceding the slave deauthorization message, the central control computer will send an inhibit command to all master decoders, again as a group. If a slave decoder is authorized

and is therefore connected to its master decoder, the inhibit command sent to the master decoder, will prevent the subsequent deauthorization message from being sent to its slave. Thus, the deauthorize signal for all slave decoders will not be retransmitted by a master decoder since it has previously been inhibited from retransmitting for a time period sufficient to avoid the retransmission of the deauthorize message to its associated slave.

Moreover, Li envisions that those slave decoders which are connected to the cable system in an unauthorized manner will receive the deauthorization message and thus will be deauthorized from then on. Only those slave decoders which are connected to a legitimate master decoder and which do not receive the deauthorization message because of the previously sent inhibit message to the master, will continue to function as legitimate slave decoders.

In view of this discussion, it appears that the combination of Li with RSA would only teach or suggest that such control signals be encrypted. However, the combination of Li and RSA would not teach or suggest the novel elements of Applicants' independent claims directed to a host-client pairing key that is used to encrypt a copy protection key used to encrypt and decrypt the program materials when shared between the host and client receivers, wherein the host-client pairing key is generated by the service provider and shared between the host receiver and client receiver in order to share the program materials between the host receiver and client receiver, and the service provider establishes the host-client pairing key for a particular combination of the host and client receivers.

Therefore, even when combined, the references teach away from Applicants' invention. Moreover, the various elements of Applicants' claimed invention together provide operational advantages over Son and the combination of Li and RSA. In addition, Applicants' invention solves problems not recognized by Son and the combination of Li and RSA.

Thus, Applicants' attorney submits that independent claims 1 and 10 are allowable over Son and the combination of Li and RSA. Further, dependent claims 2-9, 11-18, and 28-31 are submitted to be allowable over Son and the combination of Li and RSA in the same manner, because they are dependent on independent claims 1 and 10, respectively, and thus contain all the limitations of the independent claims. In addition, dependent claims 2-9, 11-18, and 28-31 recite additional novel elements not shown by Son and the combination of Li and RSA.

VI. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited.

Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

By: _____
Name: Georgann S. Grunebach, Reg. No.: 33,179
Attorney for Applicant

Date: May 8, 2007

The DIRECTV Group, Inc.
CA / LA1 / A109
P.O. Box 956
2230 E. Imperial Highway
El Segundo, CA 90245-0956

Phone: 310-964-4615